JOURNAL OF NUMBER THEORY 15, 388–405 (1982)

The Lattice of Subfields of a Radical Extension

MARIÁ ACOSTA DE OROZCO AND WILLIAM YSLAS VÉLEZ*

Department of Mathematics, University of Arizona, Tucson, Arizona 85721

Communicated by O. Taussky-Todd

Received January 1, 1981; revised October 24, 1981

DEDICATED TO HENRY B. MANN
ON THE OCCASION OF HIS 75TH BIRTHDAY

Let $x^m - a$ be irreducible over F with char $F \nmid m$ and let α be a root of $x^m - a$. The purpose of this paper is to study the lattice of subfields of $F(\alpha)/F$ and to this end $C(F(\alpha)/F, k)$ is defined to be the number of subfields of $F(\alpha)$ of degree k over F. $C(F(\alpha)/F, p^n)$ is explicitly determined for p a prime and the following structure theorem for the lattice of subfields is proved. Let N be the maximal normal subfield of $F(\alpha)$ over F and set $n = |N : F|$, then $C(F(\alpha)/F, k) = C(F(\alpha)/F, (k, n)) = C(N/F, (k, n))$. The irreducible binomials $x^s - b$, $x^s - c$ are said to be equivalent if there exist roots $\beta^s = b$, $\gamma^s = a$ such that $F(\beta) = F(\gamma)$. All the mutually inequivalent binomials which have roots in $F(\alpha)$ are determined. Finally these results are applied to the study of normal binomials and those irreducible binomials $x^{2^e} - a$ which are normal over F (char $F \neq 2$) together with their Galois groups are characterized.

1. INTRODUCTION: RESULTS AND NOTATION

Let L/F be a finite field extension. In this paper we shall study the lattice of subfields of the extension L/F, in the special case where $L = F(\alpha)$, α a root of the irreducible $x^m - a$, where char $F \nmid m$.

In the following, if $K \supset F$, then by a subfield of K we shall mean a subfield of K that contains F.

Let $C(F(\alpha)/F, k)$ be the number of subfields of $F(\alpha)$ of degree k over F, and let $N \subset F(\alpha)$ be the maximal normal subfield over F.

We begin Section 2 by characterizing the extensions $F(\alpha)/F$ with $C(F(\alpha)/F, k) = 1$ for all $k \mid m$. We next show that the function C for N/F completely determines the function C for $F(\alpha)/F$. To be more precise, let $n = |N : F|$, then we shall show that

$$C(F(\alpha)/F, k) = C(F(\alpha)/F, (k, n)) = C(N/F, (k, n)).$$

* This author was supported, in part, by a National Chicano Council on Higher Education Summer Research Grant.

0022-314X/82/060388-18$02.00/0

In Section 2 we also determine $C(F(\alpha)/F, p^f)$, for p an odd prime. To determine $C(F(\alpha)/F, 2^f)$ is a bit more involved. In order to do this we have to study those extensions $F(\alpha)/F$, $m = 2^f$, where $F(\alpha)/F$ is a normal extension. Gay [1, 2] has studied these extensions and characterized the possible degrees 2^f and the form that a must have in order that $F(\alpha)/F$ be normal.

In Section 3 we study those normal extensions $F(\alpha)/F$, where $m = 2^f$ and char $F \neq 2$. We are able to generalize Gay's results, for the case $m = 2^f$ and char $F \neq 2$, and also determine the corresponding Galois groups. Using the Galois group we are then able to compute $C(F(\alpha)/F, 2^f)$.

In returning to the general case of the lattice of the subfields of $F(\alpha)$ it is easy to see that not every subfield of $F(\alpha)$ is a radical extension. Thus a natural question arises: Which of these subfields are of the form $F(b^{1/k})$ and how is b related to a?

In the case when $k = m$, this question has already been studied in [4, 10]. In relation to this question Gerst [4] has made the following definition: Let $x^m - a$, $x^m - b$ be irreducible over F, then we say that $x^m - a$, $x^m - b$ are equivalent if there exist roots $\alpha^m = a$, $\beta^m = b$ such that $F(\alpha) = F(\beta)$. Schinzel [10] has characterized when two irreducible binomials are equivalent.

In Section 4, we determine all of the mutually inequivalent binomials which have roots in $F(\alpha)$, thereby generalizing the above results of Schinzel.

Before proceeding further with the study of the lattice of subfields we shall make some firm conventions which will be in force throughout this paper.

In equations, small latin letters shall denote elements from F. The binomial $x^m - a$ is irreducible with root α and char $F \nmid m$, ζ_k will denote a primitive kth root of unity, Z_l denotes the cyclic group with l elements, and for a prime p, $p^e \| n$ means $p^e \mid n$, $p^{e+1} \nmid n$. For two sets A and B, $A \backslash B = \{a \in A, a \notin B\}$.

We shall let N denote the maximal normal subfield of $F(\alpha)$ over F and $n = |N : F|$, the degree of N over F.

2. The Lattice of Subfields

For β algebraic over F, let $O_F(\beta)$ denote the order of β in the quotient group $F(\beta)^*/F^*$. For convenience, we state the following lemma which appears as Lemma 1.5 of [3].

LEMMA 2.1. *Let $O_F(\beta) < \infty$. If, for every prime p dividing $O_F(\beta)$ we have that $\zeta_{2p} \notin F(\beta) \backslash F$, then $|F(\beta) : F| = O_F(\beta)$.*

If $C(L/F, k) = 1$, for every $k \mid |L : F|$, then we say that L/F has the unique subfield property, abbreviated, usp. We begin the study of the lattice of subfields by characterizing those extensions $F(\alpha)/F$ with the usp.

THEOREM 2.1. *The field extension $F(\alpha)/F$ has the unique subfield property iff*

(i) *for every odd prime p, $p \mid m$, $\zeta_p \notin F(\alpha)\backslash F$, and*

(ii) *if $4 \mid m$, then $\zeta_4 \notin F(\alpha)\backslash F$.*

Proof. Assume $F(\alpha)/F$ has the usp.

Let p be an odd prime, $p \mid m$. Then $|F(\alpha^{m/p}) : F| = p$. If $\zeta_p \in F(\alpha)$, then since $F(\alpha)/F$ has the usp, we have that $F(\alpha^{m/p}) = F(\zeta_p \alpha^{m/p})$, so $\zeta_p \in F(\alpha^{m/p})$, which in turn implies that $\zeta_p \in F$ since $(|F(\zeta_p) : F|, p) = 1$. Thus $\zeta_p \notin F(\alpha)\backslash F$.

If $4 \mid m$ and $\zeta_4 \in F(\alpha)\backslash F$, then $F(a^{1/2}) = F(\zeta_4)$, since these are both quadratic subfields of $F(\alpha)$ and $F(\alpha)/F$ has the usp. Thus, $F(a^{1/4})/F$ is a normal extension with Galois group $Z_2 \oplus Z_2$ (see Theorem 2.2 of [11]), so $F(\alpha) \supset F(a^{1/4})$ would contain three distinct quadratic subfields, contradicting the assumption that $F(\alpha)/F$ has the usp. Thus $\zeta_4 \notin F(\alpha)\backslash F$.

Now, assume (i) and (ii) and let $F(\alpha) \supset K$. Set $l = \min\{k : k \mid m$ and $\alpha^k \in K\}$. Then $O_K(\alpha) = l$ and $F(\alpha) \supset K \supset F(\alpha^l)$. However, for every odd prime $p \mid l$, we have that $\zeta_p \notin F(\alpha)\backslash K$ and if $4 \mid l$, then $\zeta_4 \notin F(\alpha)\backslash K$. Thus we have, by Lemma 2.1, that $|F(\alpha) : K| = l$. So we have that $|F(\alpha) : K| = l = |F(\alpha) : F(\alpha^l)|$, and $K \supset F(\alpha^l)$. This implies that $K = F(\alpha^l)$, so K is unique. ∎

THEOREM 2.2. *Let $\mathscr{P} = \{p : p \mid m$ and $\zeta_{2p} \in F(\alpha)\backslash F\}$ and set $P = 2 \cdot \prod_{p \in \mathscr{P}} p$ if $2 \in \mathscr{P}$, or $P = \prod_{p \in \mathscr{P}} p$, if $2 \notin \mathscr{P}$. Then $F(\alpha)/F(\zeta_P)$ has the usp.*

Proof. Let N be the maximal normal subfield of $F(\alpha)$, with $n = |N : F|$. Then $\zeta_n \in F(\alpha)$ and $F(\zeta_n) = F(\alpha^{m/s})$, where $s = |F(\zeta_n) : F|$, by Theorem 1 of [9]. Thus the Galois group of $F(\zeta_n)$ is either Z_s or $Z_2 \oplus Z_{s/2}$, by Theorem 2.2 of [11].

If the Galois group is Z_s then $F(\zeta_n)/F$ has the usp, so $F(\zeta_P) = F(\alpha^{m/f})$, where $f = |F(\zeta_P) : F|$. If the Galois group is $Z_2 \oplus Z_{s/2}$, then $\zeta_4 \in F(\zeta_n)\backslash F$, again by Theorem 2.2 of [11]. Then $F(\alpha^{m/2}) = F(\zeta_4)$, by Theorem 1.8 of [3], so $F(\zeta_n) \supset F(\zeta_P) \supset F(\zeta_4)$ and $F(\zeta_n)/F(\zeta_4)$ has the usp since the Galois group is $Z_{s/2}$. Thus, $F(\zeta_P) = F(\alpha^{m/f})$.

Hence, in all cases $F(\zeta_P) = F(\alpha^{m/f})$, so α satisfies the irreducible binomial $x^{m/f} - \alpha^{m/f}$ over $F(\zeta_P)$. By Theorem 2.1, since $\zeta_{2p} \in F(\alpha)$ implies $\zeta_{2p} \in F(\zeta_P)$, we have that $F(\alpha)/F(\zeta_P)$ has the usp. ∎

We next want to show that every subfield of $F(\alpha)$ is made up of subfields of prime power order. We first prove a lemma.

LEMMA 2.2. *Let $F(\alpha) \supset K$ and $p^t \mid |F(\alpha) : F|$, where p is an odd prime. If $p \nmid |K(\alpha^{m/p^t}) : K|$, then $\alpha^{m/p^t} \zeta_{p^t}^i \in K$, for some i.*

Proof. Set $\beta = \alpha^{m/p^t}$ and let $f(x) = \mathrm{Irr}(\beta, K)$. Clearly, $f(x) \mid x^{p^t} - a$, so $f(x) = \prod_{i=1}^{q}(x - \beta(\zeta_{p^t})^{j_i})$, where $q = |K(\beta) : K|$, and the constant term of $f(x)$ is $\beta^q \zeta_{p^t}^e \in K$, for some e. Since $(q, p) = 1$, we have that $uq = 1 + yp^t$, so $(\beta^q \zeta_{p^t}^e)^u = \beta^{1+yp^t} \zeta_{p^t}^{eu} = \beta a^y \zeta_{p^t}^{eu} \in K$ and since $a^y \in F \subset K$, this implies that $\beta \zeta_{p^t}^{eu} \in K$. ∎

THEOREM 2.3. *Let $F(\alpha) \supset K$ with $|K : F| = p_1^{e_1} \cdots p_s^{e_s}$. Then for each i, there exists a subfield K_i of K such that $|K_i : F| = p_i^{e_i}$ and $K = K_1 \cdots K_s$. Further,* (a) *if p_i is odd then there exists a j, depending on i, such that $K_i = F(\alpha^{m/p_i^{e_i}} \zeta_{p_i^{e_i}}^j)$ and* (b) *if $p_1 = 2$, then K_1 is the unique subfield of degree $p_1^{e_1}$ over F in K.*

Proof. Let $p^t \| |K : F|$, p an odd prime and set $\beta = \alpha^{m/p^t}$, with $p^l = O_K(\beta)$. If $l = 0$, then $F(\alpha^{m/p^t}) \subset K$. Thus, we may assume that $l > 0$.

Let $m = m_1 p^e$, $(m_1, p) = 1$. Now, $O_K(\beta^{p^{l-1}}) = p$. If $|K(\beta^{p^{l-1}}) : K| = p$, then $|K(\alpha^{m_1}) : K| = p^{e-t+l}$, which implies that $p^{e+l} \mid |K(\alpha^{m_1}) : F| \mid |F(\alpha) : F| \mid m$, a contradiction. Thus, $|K(\beta^{p^{l-1}}) : K| < p$ and this implies that $K(\beta^{p^{l-1}}) = K(\zeta_p)$. Set $T = K(\zeta_p)$ and $p^{l'} = O_T(\beta)$. If $l' > 0$, then $|T(\beta^{p^{l'-1}}) : T| = p$, so $|T(\alpha^{m_1}) : T| = p^{e-t+l'}$, and thus $p^{e+l'} \mid |T(\alpha^{m_1}) : F| \mid |F(\alpha) : F|$, a contradiction. Thus, $l' = 0$, that is, $K(\beta) = K(\zeta_p)$. Thus we have that $p \nmid |K(\alpha^{m/p^t}) : K|$, so by Lemma 2.2 we have that $\alpha^{m/p^t} \zeta_{p^t}^j \in K$, for some j depending on p.

Let $m = m_0 2^e$, $(m_0, 2) = 1$. Set $\beta = \alpha^{m_0}$ and $T = F(\beta) \cap K$, with $2^f = |T : F|$ and $2^t \| |K : F|$. Of course we want to show that $t = f$.

It is clear that $O_T(\beta) = O_K(\beta) = 2^r$. If $\zeta_4 \notin F(\beta) \backslash T$, then $\zeta_4 \notin K(\beta) \backslash K$, so $2^r = |K(\beta) : K| = |F(\beta) : T|$. But $|F(\beta) : F| = 2^e$, so $|F(\beta) : F| = 2^e = 2^{f+r}$ and $2^e \| |K(\beta) : F| = 2^{t+r}$; thus $2^e = 2^{t+r}$, so $f = t$.

If $\zeta_4 \in F(\beta) \backslash T$, then replace K by $K(\zeta_4)$ and then $T(\zeta_4) = K(\zeta_4) \cap F(\beta)$. Now apply the above argument to $T(\zeta_4)$ and $K(\zeta_4)$.

It is obvious that $F(\beta)$ is the maximal subfield of $F(\alpha)$ with degree a power of 2 over F and $F(\beta)$ contains every subfield of $F(\alpha)$ whose degree over F is a power of 2. This shows that the degree of a compositum of subfields whose degrees are powers of 2 is again a power of 2. Thus K_1 is unique. ∎

For any field L, let $\omega(L, s)$ be the number of sth roots of unity in L, where $\mathrm{char}\, L \nmid s$. That is, $\omega(L, s)$ is the number of distinct roots of $x^s - 1$ in L.

COROLLARY 2.1. *Let $p^t \mid m$, p an odd prime. Then*

(i) *if $\zeta_p \notin F(\alpha) \backslash F$, then $C(F(\alpha)/F, p^t) = 1$,*

(ii) *if $\zeta_p \in F(\alpha) \backslash F$, then $C(F(\alpha)/F, p^t) = \omega(F(\alpha), p^t)$.*

Proof. Let $m = m_1 p^e$, $(m_1, p) = 1$. If $F(\alpha) \supset K$, where $|K : F| = p^t$, then by Theorem 2.3, there exists an i such that $K = F(\alpha^{m/p^t} \zeta_{p^t}^i)$.

If $\zeta_p \notin F(\alpha)$, then $\zeta_{p^t}^i = 1$ so K is unique.

If $\zeta_p \in F$, then $O_F(\zeta_{p^t}^i) = p^l$, for some $l < t$. Then by Theorem A of [3] we have $\zeta_{p^t}^i = c(\alpha^{m_1})^{p^{e-l}}$. Thus $\alpha^{m/p^t}\zeta_{p^t}^i = c(\alpha^{m_1})^{p^{e-l}}(\alpha^{m_1})^{p^{e-t}} = c(\alpha^{m_1})^{p^{e-l}+p^{e-t}} = c(\alpha^r)^{m/p^t}$, with $r = p^{t-l} + 1$.

Thus, $K = F(\alpha^{m/p^t}\zeta_{p^t}^i) = F(\alpha^{m/p^t}) = F((\alpha^r)^{m/p^t})$, so K is unique, that is, $C(F(\alpha)/F, p^t) = 1$.

Now suppose that $\zeta_p \in F(\alpha)\backslash F$. Then the maximum number of fields with $|K : F| = p^t$ is $\omega(F(\alpha), p^t)$ by Theorem 2.3. If $F(\alpha^{m/p^t}\zeta_{p^t}^i) = F(\alpha^{m/p^t}\zeta_{p^t}^j)$, $1 \leqslant i, j \leqslant p^t$, $i \neq j$, then $\zeta_p \in F(\alpha^{m/p^t}\zeta_{p^t}^i)$, which is a contradiction since $|F(\zeta_p) : F| \nmid p^t$. Thus the $\omega(F(\alpha), p^t)$ fields of degree p^t are all distinct, that is, $C(F(\alpha)/F, p^t) = \omega(F(\alpha), p^t)$. ∎

Recall that N is the maximal normal subfield of $F(\alpha)$ and $n = |N : F|$. By Theorem 2.2 we have that $N = F(a^{1/n})$.

THEOREM 2.4. *Let* $F(\alpha) \supset K$ *and set* $d = (|K : F|, n)$, *then* $|K \cap N : F| = d$. *Further*, (i) *if* $n \mid |K : F|$, *then* K *is the unique subfield of* $F(\alpha)$ *of degree* $|K : F|$ *over* F, *and* (ii) *if* $|K : F| \mid n$, *then* $K \subset N$.

Proof. We first consider the case $m = 2^e$. Set $n = 2^k$. If $\zeta_4 \notin F(\alpha)\backslash F$, then $F(\alpha)/F$ has the usp, and the result is obvious. So we may assume that $\zeta_4 \in F(\alpha)\backslash F$. Again, $F(\alpha)/F(\zeta_4)$ has the usp, so if $\zeta_4 \in K$, then K is unique. Thus, we may assume that $\zeta_4 \notin K$. Let $|K : F| = 2^s$, then $K(\zeta_4) = F(\alpha^{2^{e-s-1}})$.

Let us first consider the case $s < k$. We wish to show that $K \subset N$.

Let $K \cap N = F(\theta)$ and define

$$2^l = \min\{2^i : 2^i \mid 2^e \text{ and } \alpha^{2^i} \in K\},$$

$$2^h = \max\{2^i : 2^i \mid 2^e \text{ and } K \subset F(\alpha^{2^i})\}.$$

Clearly, $h = e - s - 1$ and since $F(\alpha^{2^{e-s-1}}) = F(\zeta_4) \not\subset K$, we have that $l = e$. Since $(2^{e-k}, 2^e) = 2^{e-k} = (2^{e-k}, 2^{e-s-1})$ we have that $K = F(\theta, \alpha^{2^e}) = F(\theta)$; thus $K \subset N$ (that $K = F(\theta, \alpha^{2^e})$ is obtained by a slight generalization of Theorem 2 of [9], that is, by replacing $F(\zeta_n)$ by $F(a^{1/n})$ in Theorem 2 of [9]).

If $s \geqslant k$, then $|K(\zeta_4) : F| = 2^{s+1} > 2^k$. However, $K(\zeta_4) = F(\alpha^{2^{e-s-1}})$ and $O_K(\alpha^{2^{e-s-1}}) = 2^{s+1}$. But $K(\alpha^{2^{e-s-1}})/K$ is normal, since it is quadratic; hence by Theorem 3 of [9], we have that $\zeta_{2^{s+1}} \in F(\alpha)$, which contradicts the maximality of N, since $s + 1 > k$. Thus, if $s \geqslant k$, $\zeta_4 \in K$ so K is unique.

Now, let us return to the general situation. Write $n = 2^k n_0$, $(2, n_0) = 1$, $|K : F| = s = 2^{e_1}s_0$, $(s_0, 2) = 1$. Of course, if $F(a^{1/2^k})$ is the maximal normal subfield of $F(\alpha^{m_0})$ then $2^k \parallel n$ and $F(a^{1/2^k}) \subset N$.

Let K_1 be the unique subfield of K with $2^{e_1} = |K_1 : F|$. If $e_1 \leqslant k$, then $K_1 \subset F(a^{1/2^k}) \subset N$, by the preceding case ($m = 2^e$). If $e_1 > k$, then $K_1 \supset F(a^{1/2^k})$ and K_1 is the unique subfield of $F(\alpha)$ of degree 2^{e_1} over F.

Let $p^t \parallel |K : F|$, p odd. Then, for some j, $\alpha^{m/p^t}\zeta_{p^t}^j \in K$. If $p^t \mid n$, then

$\alpha^{m/p^t}\zeta_{p^t}^j \in N$, so $p^t \mid [K \cap N : F]$. If $p^c \mid n_0$, $c < t$, then $(\alpha^{m/p^t}\zeta_{p^t}^j)^{p^{t-c}} = \alpha^{m/p^c}\zeta_{p^t}^j \in N$; thus $p^c \mid [N \cap K : F]$.

Thus, we have shown that if $d = ([K : F], n)$, then $d = [K \cap N : F]$.

Now, suppose $n \mid [K : F]$, then $K \supset F(a^{1/n}) \supset F(\zeta_n)$, so K is unique, by Theorem 2.2.

Assertion (ii) follows trivially from the first part of the theorem. ∎

LEMMA 2.3. *Let $F(\alpha) \supset K$, $[K : F] = cp^t$, $(c, p) = 1$, p odd. Then there exist subfields T_1, T_2 of K with $[T_1 : F] = c$, $[T_2 : F] = p^t$. If $\zeta_p \notin K$, then T_1, T_2 are the unique subfields of K of degree c and p^t, respectively.*

Proof. By Theorem 2.3, $T_2 = F(\alpha^{m/p^t}\zeta_{p^t}^i)$ for some i with $\zeta_{p^t}^i \in F(\alpha)$, $1 \leqslant i \leqslant p^t$. If $\alpha^{m/p^t}\zeta_{p^t}^j \in K$, $1 \leqslant j \leqslant p^t$, $i \neq j$, then this would imply that $\zeta_p \in K$, contrary to assumption. Hence T_2 is unique.

Let $c = 2^{e_1}c_1$, $(2, c_1) = 1$ and let K_1 be the unique (by Theorem 2.3) subfield of K of degree 2^{e_1} over F. Then since $[K : T_1] = p^t$, p odd where $[T_1 : F] = c$ and $T_1 \subset K$, we must have that $K_1 \subset T_1$ and by Theorem 2.3, we have that $T_1 = K_1(\alpha^{m/c_1}\zeta_{c_1}^j)$. If $T_3 \subset K$ with $[T_3 : F] = c$, then the above argument applied to T_3 yields $T_3 = K_1(\alpha^{m/c_1}\zeta_{c_1}^l)$, with $1 \leqslant j$, $l \leqslant c_1$. If $T_1 \neq T_3$, then $T_1 T_3 \neq T_1$. However, $T_1 T_3 = T_1(\zeta_{c_1}^l)$, so $T_1 T_3 / T_1$ is an abelian extension. Also K/T_1 is of degree p^t and K/T_1 has the usp by Theorem 2.1. Thus $T_1 T_3 = T_1((\alpha^{m/p^t}\zeta_{p^t}^i)^{p^{t-d}}) = T_1(\alpha^{m/p^d}\zeta_{p^c}^i)$, where $p^d = [T_1 T_3 : T_1]$. But the extension being normal implies that $\zeta_p \in T_1 T_3 \subset K$, contradicting the assumption that $\zeta_p \notin K$. Thus $T_1 = T_3$, so T_1 is unique. ∎

COROLLARY 2.2. *Let $cp^t \mid m$, p odd and $(c, p) = 1$ and suppose that s is the number of subfields of $F(\alpha)$ of degree c over F which do not contain ζ_p. Then the number of subfields of degree cp^t which do not contain ζ_p is $s\omega(F(\alpha), p^t)$.*

Proof. Let $L_1, \ldots, L_s$ be all of the subfields of $F(\alpha)$ of degree c over F with $\zeta_p \notin L_i$. Let $T_1, \ldots, T_\omega$, $\omega = \omega(F(\alpha), p^t)$ be those subfields of $F(\alpha)$ of degree p^t over F. Then by Lemma 2.3, $L_{i_1} T_{j_1} = L_{i_2} T_{j_2}$, iff $i_1 = i_2$, $j_1 = j_2$. Thus, the Corollary follows. ∎

COROLLARY 2.3. *Let $k \mid m$ and let $k = k_1 k_2$, where k_1 is the maximal divisor of k with $(k_1, n) = 1$ (n is the degree of the maximal normal subfield of $F(\alpha)$). Then $C(F(\alpha)/F, k) = C(F(\alpha)/F, k_2)$.*

Proof. If $p \mid k_1$, then $\zeta_p \notin F(\alpha)$, so if $p^t \parallel k_1$, then $\omega(F(\alpha), p^t) = 1$. Write $k = p^t k_3$. Then, by Corollary 2.2, $C(F(\alpha)/F, k) = C(F(\alpha)/F, k_3)\,\omega(F(\alpha), p^t) = C(F(\alpha)/F, k_3)$.

The corollary now follows easily by inducting on the number of prime factors of k_1. ∎

THEOREM 2.5. *Let N be the maximal normal subfield of $F(\alpha)$ with $n = [N : F]$. For $k \mid m$ set $d = (k, n)$. Then $C(F(\alpha)/F, k) = C(F(\alpha)/F, d) = C(N/F, d)$.*

Proof. We first prove the following: Let $n = p^t n_0$, $(p, n_0) = 1$ and suppose that $k = p^{t+l}k_0$, $(p, k_0) = 1$. Then $C(F(\alpha)/F, p^{t+l}k_0) = C(F(\alpha)/F, p^t k_0)$. If $t = 0$, this follows from Corollary 2.3. Thus we may assume that $t > 0$ and $l > 0$.

For $b \mid m$, set $f_p(b) = |\{K \subset F(\alpha)\colon [K : F] = b \text{ and } \zeta_p \in K\}|$ and $g_p(b) = |\{K \subset F(\alpha)\colon [K : F] = b \text{ and } \zeta_p \notin K\}|$. Thus $C(F(\alpha)/F, b) = f_p(b) + g_p(b)$.

Since $p^t \| n$ and $l > 0$, we have that $\zeta_{p^t} \in N$, $\zeta_{p^{t+1}} \notin F(\alpha)$, so $p^t = \omega(F(\alpha), p^t) = \omega(F(\alpha), p^{t+l})$. Then by Corollary 2.2 we have $g_p(p^t k_0) = g_p(k_0)\,\omega(F(\alpha), p^t) = g_p(k_0)\,\omega(F(\alpha), p^{t+l}) = g_p(p^{t+l}k_0)$. Hence, it only remains to show that $f_p(p^t k_0) = f_p(p^{t+l}k_0)$.

Claim 1. Let $[L : F] = p^c k_0$, $c \geqslant t$, $\zeta_p \in L$, and $T \subset L$ be such that $[T : F] = k_0$, then $L = T(\alpha^{m/p^c})$.

Proof of Claim 1. By Theorem 2.3 there exists $L_1 \subset L$ such that $p^c = [L_1 : F]$. First assume $p = 2$. If $2^e \| m$, then $F(\alpha^{m/2^e}) \supset L_1 \supset F(\alpha^{m/2^t})$, where $F(\alpha^{m/2^t})$ is the maximal normal subfield of $F(\alpha^{m/2^e})$, thus $L_1 = F(\alpha^{m/2^c})$, by Theorem 2.2. Thus $L = L_1 \cdot T = T(\alpha^{m/2^c})$.

For p odd, if $\zeta_p \in F$, then $C(F(\alpha)/F, p^c) = 1$, so $L_1 = F(\alpha^{m/p^c})$ and $L = L_1 \cdot T = T(\alpha^{m/p^c})$. If $\zeta_p \in L \backslash F$, then $\zeta_p \in T$ since $[L : T] = p^c$. However, by Corollary 1.10 of [3], we have that $F(\zeta_p) = F(\zeta_{p^t}) \subset T$. By Theorem 2.3, $L_1 = F(\alpha^{m/p^c}\zeta_{p^t}^j)$, so $L = L_1 \cdot T = T(\alpha^{m/p^c}\zeta_{p^t}^j) = T(\alpha^{m/p^c})$ since $\zeta_{p^t} \in T$, and Claim 1 is proven.

Set $f = f_p(p^t k_0)$ and let $L_1, \ldots, L_f$ be the f distinct subfields of $F(\alpha)$ of degree $p^t k_0$ with $\zeta_p \in L_i$, $1 \leqslant i \leqslant f$. Let $T_i \subset L_i$ be such that $[T_i : F] = k_0$. Then by Claim 1, $L_i = T_i(\alpha^{m/p^t})$.

Let $[L : F] = p^{t+l}k_0$, $\zeta_p \in L$, $T \subset L$ be such that $[T : F] = k_0$. Then by Claim 1, $L = T(\alpha^{m/p^{t+l}}) \supset T(\alpha^{m/p^t}) = L_i$, for some i. Hence $T_i \subset L$, so we may assume that $L = T_i(\alpha^{m/p^{t+l}})$. This shows that $f(p^{t+l}k_0) \leqslant f = f(p^t k_0)$.

The proof will be complete provided we can show that $T_i(\alpha^{m/p^{t-1}}) = T_j(\alpha^{m/p^{t+l}})$ implies $i = j$. However, as in the proof of Lemma 2.3, we have that if $T_i \neq T_j$, then $T_i T_j / T_i$ is an abelian extension of degree a power of p. Thus $T_i T_j$ is contained in the maximal normal sub-extension of the extension $T_i(\alpha^{m/p^{t+l}})/T_i$. However, since $\zeta_{p^t} \in F(\alpha)$, $\zeta_{p^{t+1}} \notin F(\alpha)$, the maximal normal sub-extension of $T_i(\alpha^{m/p^{t+l}})/T_i$ is $T_i(\alpha^{m/p^t})$. Hence, $T_i T_j \subset T_i(\alpha^{m/p^t})$, so $T_j \subset T_i(\alpha^{m/p^t})$, which implies that $L_i = T_i(\alpha^{m/p^t}) = T_j(\alpha^{m/p^t}) = L_j$, so $i = j$. This proves that $C(F(\alpha)/F, p^t k_0) = C(F(\alpha)/F, p^{t+l}k_0)$, thus $C(F(\alpha)/F, k) = C(F(\alpha)/F, d)$. However, $d \mid n$ and by Theorem 2.4 we have that $C(F(\alpha)/F, d) = C(N/F, d)$. ∎

We would like to conclude this section by making some remarks about radical extensions in general.

Theorem 2.5 reduces the computation of $C(F(\alpha)/F, k)$ to the normal case (studied in [1, 2, 7, 11]), where C can be calculated by determining $G = \mathrm{Gal}(F(a^{1/n})/F)$ and the number of subgroups of G of index k, though both are hard problems in general.

However, Theorem 2.2 does allow us to say something about $\mathrm{Gal}(F(\alpha)/F)$.

COROLLARY 2.4. *Let $x^m - a$ be normal and let P be defined as in Theorem 2.2 with $f = [F(\zeta_P) : F]$. Then $G = \mathrm{Gal}(F(\alpha)/F)$ contains a cyclic normal subgroup H of index f such that $G/H \cong Z_2 \oplus Z_{f/2}$ if $4 \mid P$ and $4 \mid f$, and G/H is cyclic otherwise.*

Proof. Since $F(\alpha)/F(\zeta_P)$ is normal with the usp, let $H = \mathrm{Gal}(F(\alpha)/F(\zeta_P))$, then H is cyclic and $G/H = \mathrm{Gal}(F(\zeta_P)/F)$. The rest follows from Theorem 2.2 of [11]. ∎

THEOREM 2.6. *Let $F(\alpha)/F$ be normal with $m = 2^e m_0$, $(2, m_0) = 1$ and let $G = \mathrm{Gal}(F(\alpha)/F)$, $H_1 = \mathrm{Gal}(F(\alpha)/F(\alpha^{m_0}))$, $H_2 = \mathrm{Gal}(F(\alpha)/F(\alpha^{2^e}))$. Then $|H_1| = m_0$, $|H_2| = 2^e$, H_1 is a normal subgroup of G, H_2 contains a cyclic normal subgroup of index 2 and G is a semi-direct product of H_1 and H_2. Further every p-Sylow subgroup of H_1 is cyclic.*

Proof. Since $F(\alpha^{m_0})$ is the unique subfield of degree 2^e, H_1 is normal. Further, since $(|H_1|, |H_2|) = 1$, we have that $H_1 \cap H_2 = 1$. Also $G = H_1 \cdot H_2$, so G is a semi-direct product of H_1 and H_2.

For G_p, a p-Sylow subgroup of G, p odd, let F_p be the fixed field of G_p. Then $2^e \| [F_p : F]$, which implies that $F(\alpha^{m_0}) \subset F_p$. Thus, $G_p \subset H_1$.

Let $p^{e_1} \| m$, then $\zeta_{p^{e_1}} \in F(\alpha)$. Since $|F(\alpha) : F_p] = p^{e_1}$, we must have that $\zeta_p \in F_p$. However, $F(\alpha) = F_p(\alpha^{m/p^{e_1}})$ and since $\zeta_p \in F_p$, we have that $F(\alpha)/F_p$ has the usp. Thus $G_p = \mathrm{Gal}(F/F_p)$ is cyclic.

Finally, we wish to prove that H_2 contains a cyclic subgroup of index 2. Now, α satisfies the irreducible binomial $x^{2^e} - \alpha^{2^e}$ over $F(\alpha^{2^e})$. If $\zeta_4 \notin F(\alpha) \backslash F$, then $F(\alpha)/F(\alpha^{2^e})$ has the usp, so H_2 is cyclic. If $\zeta_4 \in F(\alpha) \backslash F$, then $F(\alpha^{2^{e-1}}, \zeta_4) = F(\alpha^{2^{e-1}})$ and $F(\alpha)/F(\alpha^{2^{e-1}})$ has the usp; thus $F(\alpha)/F(\alpha^{2^{e-1}})$ has cyclic Galois group. Thus, in either case, H_2 has a cyclic normal subgroup of index 2. ∎

In [1], Gay studied normal radical extensions over real fields. For a real field we have that $\omega(F, m) = 1$ or 2, since the only roots of unity are ± 1. If $\omega(F, m) = 1$ or 2, then we can say more about the group H_1.

COROLLARY 2.5. *Let $F(\alpha)/F$ be normal with $m = 2^e m_0$, $(2, m_0) = 1$, and $H_1 = \mathrm{Gal}(F(\alpha)/F(\alpha^{m_0}))$. If $\omega(F, m) = 2^c$, $c \geqslant 0$, then H_1 is cyclic.*

Proof. By Theorem 2.2, we have that $F(\zeta_m) = F(\alpha^{m/r})$, where $r = |F(\zeta_m) : F|$. If $p \mid r$, then $F(\zeta_m) \supset F(\alpha^{m/p})$ and $F(\alpha^{m/p})$ is also abelian; thus $\zeta_p \in F$, so $p = 2$ since $\omega(F, m) = 2^c$, $c \geqslant 0$. Thus, $F(\zeta_m) \subset F(\alpha^{m_0})$, so $F(\alpha)/F(\alpha^{m_0})$ has the usp; thus H_1 is cyclic. ∎

We have yet to calculate $C(F(\alpha)/F, 2^t)$. By the above results we only have to calculate this function when $F(\alpha)/F$ is normal. In this case, $\mathrm{Gal}(F(\alpha)/F)$ has a cyclic normal subgroup of index 2, by Theorem 2.6. For $m = 2^e$, explicitly characterizing $\mathrm{Gal}(F(\alpha)/F)$ is managable and this we shall do in the following section.

3. Normal Binomials $x^{2^e} - a$ and Their Galois Groups

Throughout this section $m = 2^e$, $x^{2^e} - a$ will be normal and G will denote the Galois group of $F(\alpha)/F$. Let F^* denote the multiplicative group of non-zero elements and $T(F(\alpha)^*/F^*)$ the torsion subgroup of the quotient group $F(\alpha)^*/F^*$. For a prime p, $T_p(F(\alpha)^*/F^*)$ denotes the subgroup of $T(F(\alpha)^*/F^*)$ whose elements have orders which are powers of p.

If $\zeta_4 \in F$, then $F(\alpha)/F$ has the usp, so G is cyclic. Thus, we may assume that $\zeta_4 \in F(\alpha) \backslash F$. Then, $H = \mathrm{Gal}(F(\alpha)/F(\zeta_4))$ is cyclic since $F(\alpha)/F(\zeta_4)$ has the usp, and $G/H = Z_2$. If G is abelian, then $G = Z_{2^{e-1}} \oplus Z_2$, by Theorem 2.2 of [11]. So, we shall assume that G is not abelian. Groups which have a cyclic subgroup of index 2 have been characterized (see p. 150 of [12]). There are four non-abelian groups of this kind and the following is the characterization.

Let $G = \langle A, B \rangle$, where $|G| = 2^e$ and $\langle A \rangle$ is a cyclic subgroup of order 2^{e-1}. Then the four isomorphism types are given in the list $\mathcal{L}$:

$\mathcal{L}$: (I) $e \geqslant 3$, $A^{2^{e-1}} = 1$, $B^2 = A^{2^{e-2}}$, $BAB^{-1} = A^{-1}$, generalized quaternion group.

(II) $e \geqslant 3$, $A^{2^{e-1}} = 1$, $B^2 = 1$, $BAB^{-1} = A^{-1}$, dihedral group.

(III) $e \geqslant 4$, $A^{2^{e-1}} = 1$, $B^2 = 1$, $BAB^{-1} = A^{-1+2^{e-2}}$.

(IV) $e \geqslant 4$, $A^{2^{e-1}} = 1$, $B^2 = 1$, $BAB^{-1} = A^{1+2^{e-2}}$.

By the preceding remarks, we have that G is isomorphic to one of these groups, and in fact we shall show that each of these groups actually occurs as the Galois group, $\mathrm{Gal}(F(\alpha)/F)$, for some α and some field F.

Let $\eta_{2^t} = \zeta_{2^t} + \zeta_{2^t}^{-1}$. For F, let $T = \max\{t : \eta_{2^t} \in F\}$ if the set is finite, otherwise set $T = \infty$. Note that $\eta_{2^2} = 0$ and $\eta_{2^3} = \sqrt{2}$.

Lemma 3.1. *Suppose that $m = 2^e$, $F(\alpha)/F$ is normal, $\zeta_4 \notin F$, and $|F(\zeta_{2^e}) : F| = 2$, where $e \geqslant 3$. Let τ be the non-trivial automorphism of $F(\zeta_{2^e})/F$. Then $\tau(\zeta_{2^e}) = \zeta_{2^e}^{-1}$ or $-\zeta_{2^e}^{-1}$. Further,*

(a) *if* ζ_{2^e} *and* $\zeta_{2^e}^{-1}$ *are conjugates, then* G *is the dihedral group,*

(b) *if* ζ_{2^e} *and* $-\zeta_{2^e}^{-1}$ *are conjugates, then* G *is the generalized quaternion.*

Proof. Since $\tau(\zeta_{2^e})\,\zeta_{2^e}$ is a root of unity in F, we must have that $\tau(\zeta_{2^e})\,\zeta_{2^e} = \pm 1$, so $\tau(\zeta_{2^e}) = \pm\zeta_{2^e}^{-1}$.

The group $G = \mathrm{Gal}(F(\alpha)/F)$ has 2^e automorphisms, which are given by $\sigma_i(\alpha) = \alpha\zeta_{2^e}^i$, $0 \leqslant i \leqslant 2^e - 1$. Clearly, $\langle\sigma_2\rangle = \mathrm{Gal}(F(\alpha)/F(\zeta_4))$; thus $\langle\sigma_2\rangle$ is cyclic of order 2^{e-1}, and since $\sigma_1 \notin \langle\sigma_2\rangle$, the restriction of σ_1 to $F(\zeta_4)$ is τ. Remarks (a) and (b) now follow as easy calculations. ∎

COROLLARY 3.1. *Suppose* $m = 2^e$, $F(\alpha)/F$ *is normal,* $\zeta_4 \notin F$, *and* $[F(\zeta_{2^e}) : F] = 2$, $e \geqslant 3$. *If* $e \leqslant T$, *then* G *is the dihedral group. If* $T < \infty$, $e = T + 1$ *and* $\zeta_4\eta_{2^T} \in F$, *then* G *is the generalized quaternion.*

Proof. If $e \leqslant T$, then $\eta_{2^e} = \zeta_{2^e} + \zeta_{2^e}^{-1} \in F$, so ζ_{2^e}, $\zeta_{2^e}^{-1}$ are conjugates and Lemma 3.1 then gives that G is the dihedral group.

If $e = T + 1$ and $\zeta_4\eta_{2^T} \in F$, then $[F(\zeta_{2^T}) : F] = 2$, and ζ_{2^e}, $-\zeta_{2^e}^{-1}$ are conjugates over F, so G is the generalized quaternion group. ∎

LEMMA 3.2. *Suppose that* $m = 2^e$, $e \geqslant 3$, $F(\alpha)/F$ *is normal,* $\zeta_4 \notin F$, *and* $\zeta_8 \in F(\zeta_4)$. *Let* G' *be the commutator of* G, *then* $G/G' \cong Z_2 \oplus Z_2$.

Proof. Let K be the maximal abelian subfield of $F(\alpha)$, then $\zeta_4 \in K$ and $K = F(\alpha^{2^s})$, where $2^s = |F(\alpha) : K|$. We shall show that $s = e - 2$ by showing that $F(a^{1/8})$ is not abelian. By a Theorem of Schinzel (see Theorem 2.1 of [11]), $x^8 - a$ has abelian Galois group iff $a^2 = b_1^8$, for some $b_1 \in F$. Thus, $a = \pm b_1^4$, however, $a \neq b_1^4$ since $a \notin F^2$; thus $a = -b_1^4$ and $x^4 - a = x^4 + b_1^4$ is reducible since $\zeta_8 \in F(\zeta_4)$, which contradicts the irreducibility of $x^8 - a$. ∎

LEMMA 3.3. *If* $T < \infty$ *and* $\zeta_4\eta_{2^T} \in F$, *then* $\zeta_{2^{T+2}} \notin F(\alpha)$.

Proof. Clearly $\zeta_{2^{T+1}} \in F(\zeta_4)$. Further, by Theorem A of [3], we have that $T_2(F(\zeta_4)^*/F^*) = \langle\zeta_{2^{T+1}}F^*\rangle = Z_{2^T}$. Also, by the same theorem, $T_2(F(a^{1/4})^*/F^*) = Z_2 \oplus Z_{2^T}$. If $\zeta_{2^{T+2}} \in F(a^{1/4})$, then there would be an element of order 2^{T+1} in $F(a^{1/4})$, which is a contradiction, thus $\zeta_{2^{T+2}} \notin F(\alpha)$. ∎

Now, let us consider the case where $\zeta_4\eta_{2^{T+1}} \notin F$, $T \geqslant 3$.

LEMMA 3.4. *Suppose* $T \geqslant 3$, $\zeta_4\eta_{2^{T+1}} \notin F$, *then* $e \leqslant T + 1$. *Further,* $e = T + 1$ *iff* $a = -(2 + \eta_{2^T})^2\, c^4$, *for some* $c \in F$.

Proof. Since $\zeta_4\eta_{2^{T+1}} \notin F$, we have that $[F(\zeta_{2^{T+2}}) : F] = 8$, however, $|G/G'| = 4$ by Lemma 3.2, thus $e \leqslant T + 1$.

Clearly, $\zeta_{2^{T+1}} \in F(\alpha)$ iff $F(\zeta_{2^{T+1}}) = F(a^{1/4})$. If $F(\zeta_{2^{T+1}}) = F(a^{1/4})$, then $\zeta_{2^{T+1}} = \gamma a^{1/4}$, $\gamma \in T_2(F(\zeta_4)^*/F^*)$, and $O_F(\gamma) = 2^T$; thus $\gamma = (1 + \zeta_{2^T})^j d$, j odd and $d \in F$. So $\zeta_{2^{T+1}} = d(1 + \zeta_{2^T})^j a^{1/4}$, $\zeta_{2^{T+1}}^2 = \zeta_{2^T} = d^2 \zeta_{2^T}^j (2 + \eta_{2^T})^j a^{1/2}$. Therefore, $a = -c^4(2 + \eta_{2^T})^2$, for some $c \in F$. Conversely, the binomial $x^4 - a = x^4 + c^4(2 + \eta_{2^T})^2$ has $a^{1/4} = c\zeta_8 \eta_{2^{T+1}}$ as a root and $F(a^{1/4}) = F(\zeta_4, \eta_{2^{T+1}}) = F(\zeta_{2^{T+1}})$. ∎

LEMMA 3.5. *Suppose* $\zeta_4 \eta_{2^{T+1}} \notin F$, $T \geqslant 3$, $a = -(2 + \eta_{2^T})^2$, *and* $e = T + 1$, *then* $G = \mathrm{Gal}(F(\alpha)/F)$ *is group* III *in* $\mathscr{L}$.

Proof. Let $\sigma_i(\alpha) = \alpha \zeta_{2^{T+1}}^i$, then $\langle \sigma_2 \rangle = \mathrm{Gal}(F(\alpha)/F(\zeta_4))$ and σ_1 restricted to $F(\zeta_4)$ is the non-trivial automorphism of $F(\zeta_4)/F$. Thus $\sigma_1(\zeta_{2^T}) = \zeta_{2^T}^{-1}$. Since $\sigma_1(\alpha) = \alpha \zeta_{2^{T+1}}$, we have that $\sigma_1(a^{1/4}) = \zeta_4 a^{1/4}$. However, $a^{1/4} = \zeta_8 \eta_{2^{T+1}}$; thus $\sigma_1(a^{1/4}) = \zeta_8^{-1} \sigma_1(\eta_{2^{T+1}})$, which in turn implies that $\sigma_1(\eta_{2^{T+1}}) = -\eta_{2^{T+1}}$. This in turn implies that σ_1 fixes $\zeta_4 \eta_{2^{T+1}}$. Thus, σ_1 restricted to $F(a^{1/4})$ is the non-trivial automorphism of $F(a^{1/4})/F(\zeta_4 \eta_{2^{T+1}})$. Now, $\zeta_4 \notin F(\zeta_4 \eta_{2^{T+1}})$ and $\zeta_{2^{T+1}}, -\zeta_{2^{T+1}}^{-1}$ are conjugate over $F(\zeta_4 \eta_{2^{T+1}})$; thus, $\sigma_1(\zeta_{2^{T+1}}) = -\zeta_{2^{T+1}}^{-1}$, which implies that $\sigma_1^2(\alpha) = -\alpha = \sigma_2^{2^T}(\alpha)$, $\sigma_1^{-1}(\alpha) = -\alpha \zeta_{2^{T+1}}$. Also $\sigma_2(\zeta_{2^{T+1}}) = -\zeta_{2^{T+1}}$, and using the above information we obtain that $\sigma_1 \sigma_2 \sigma_1^{-1}(\alpha) = \sigma_2^{-1+2^T}(\alpha)$.

Consider the element $\sigma_1 \sigma_2$. It is easy to show that $(\sigma_1 \sigma_2)^2 = 1$ and $(\sigma_1 \sigma_2)\sigma_2(\sigma_1 \sigma_2)^{-1} = \sigma_2^{-1+2^T}$. Hence G is group III of $\mathscr{L}$. ∎

We are only left with the case $T = 2$, $\zeta_4 \eta_{2^3} \notin F$.

LEMMA 3.6. *If* $T = 2$, $\zeta_4 \eta_{2^3} \notin F$, *and* $e \geqslant 4$, *then* G *is either abelian or it is group* IV *of* $\mathscr{L}$.

Proof. We have already considered the case when G is abelian. Thus we can assume that G is not abelian, that is, $(1) \neq G'$.

From the fact that $T = 2$, $\zeta_4 \eta_{2^3} \notin F$, we have that $|F(\zeta_{2^e}) : F| = 2^{e-1}$, thus $F(\alpha^2) = F(\zeta_{2^e})$ is an abelian extension of F. This in turn implies that $G' = \mathrm{Gal}(F(\alpha)/F(\zeta_{2^e}))$. However, $\langle \sigma_2 \rangle = \mathrm{Gal}(F(\alpha)/F(\zeta_4))$, where $\sigma_i(\alpha) = \alpha \zeta_{2^e}^i$, thus $G' = \langle \sigma_2^{2^{e-2}} \rangle$.

Now, since G is not abelian, $|\sigma_1, \sigma_2| \neq 1$, so $|\sigma_1, \sigma_2| = \sigma_2^{2^{e-2}}$, which yields that $\sigma_1 \sigma_2 \sigma_1^{-1} = \sigma_2^{1+2^{e-2}}$. If $\sigma \in G$, $\sigma \notin \langle \sigma_2 \rangle$, then $\sigma = \sigma_1 \sigma_2^j$, for some j, and $\sigma_1 \sigma_2^j \sigma_2 (\sigma_1 \sigma_2^j)^{-1} = \sigma_1 \sigma_2 \sigma_1^{-1} = \sigma_2^{1+2^{e-2}}$, since $\langle \sigma_2 \rangle$ is abelian. Thus, G cannot be of type I, II, or III because $\sigma \sigma_2 \sigma^{-1} \neq \sigma_2^{1+2^{e-2}}$, for all $\sigma \notin \langle \sigma_2 \rangle$, thus G must be of type IV. ∎

The preceding results allow us to obtain necessary and sufficient conditions for an irreducible binomial $x^{2^e} - a$ to be normal over F for arbitrary fields with $\mathrm{char}\, F \neq 2$. We shall, however, postpone this development until the end of the next section. It is not difficult to see that each of the groups from list $\mathscr{L}$ actually appears as the Galois group for

some radical extension $F(\alpha)/F$, $\alpha^{2^c} = a$. This shall be proven explicitly in Theorem 4.3, however, for the rest of the section we shall assume that this has been proven. The reader can see that the following results are not used in Section 4.

We shall next apply these results to the problem of computing $C(F(\alpha)/F, 2^t)$. To do this it is sufficient to count the number of subgroups that each of the groups from list $\mathscr{L}$ has. We shall accomplish this in the following series of lemmas.

LEMMA 3.7. *Let G be any of the groups in $\mathscr{L}$, then G contains exactly three subgroups of index 2 and every other proper subgroup is contained in one of these.*

Proof. Since G is a 2-group generated by 2 elements the number of subgroups of index 2 is 3 (see p. 123 of [8]). The second part is Corollary 4.2.2 of [5]. ∎

LEMMA 3.8. *If G is one of the groups in $\mathscr{L}$, then the three different subgroups of index 2 in G are $H_1 = \langle A \rangle$, $H_2 = \langle A^2, B \rangle$, and $H_3 = \langle A^2, BA \rangle$. Furthermore, if $H < G$, $|H| = 2^{e-c}$, then $A^{2^c} \in H$.*

Proof. The Lemma follows by an easy calculation. ∎

LEMMA 3.9. *Let H_i, $i = 1, 2, 3$, be as in Lemma 3.8. Then:*

(i) *If $e = 3$ and G is quaternion, then H_2 and H_3 are both cyclic. If $e = 3$ and G is dihedral, then H_2 and H_3 are both isomorphic to $Z_2 \oplus Z_2$.*

(ii) *If $e \geqslant 4$ and G is of type* I *or* II, *then both H_2 and H_3 are of types* I *and* II, *respectively.*

(iii) *If $e \geqslant 4$ and G is of type* III, *then H_2 is a dihedral group and H_3 is a generalized quaternion group.*

(iv) *If $e \geqslant 4$ and G is of type* IV, *then $H_2 = Z_2 \oplus Z_{2^{e-2}}$ and $H_3 = Z_{2^{e-1}}$.*

Proof. A simple calculation verifies (i), (ii), and (iii). To prove (iv) one observes that $BA^2 = BA \cdot A = A^{1+2^{e-2}}BA = A^{1+2^{e-2}}BAB^{-1}B = A^{1+2^{e-2}+1+2^{e-2}}B = A^2B$; thus H_2 is abelian. However, $B \notin \langle A \rangle$, so $H_2 = Z_2 \oplus Z_{2^{e-2}}$. To show that H_3 is cyclic, one observes that $(BA)^2 = BABA = BAB^{-1}B^2A = A^{1+2^{e-2}}A = (A^2)^{1+2^{e-3}}$, however, since $1 + 2^{e-3}$ is odd, we have that $\langle A^2 \rangle = \langle (A^2)^{1+2^{e-3}} \rangle$; thus $H_3 = \langle AB \rangle$ is cyclic. ∎

Now we sketch the proof of the theorem that will give us $C(F(\alpha)/F, 2^k)$, for $1 \leqslant k \leqslant e$.

THEOREM 3.1. *Let* $x^{2^e} - a$ *be irreducible and normal, with* $\mathrm{Gal}(F(\alpha)/F) = G$, *where* $\alpha^{2^e} = a$ *and* $\mathrm{char}\, F \neq 2$. *Then*:

(1) *If* G *is of type* IV, $C(F(\alpha)/F, 2^k) = 3$, $1 \leqslant k \leqslant e-1$.

(2) *If* G *is of type* I, II, *or* III, *then* $C(F(\alpha)/F, 2^k) = 2^k + 1$, *for* $1 \leqslant k \leqslant e-2$.

If G *is of type* I, *then* $C(F(\alpha)/F, 2^{e-1}) = 1$.

If G *is of type* II, *then* $C(F(\alpha)/F, 2^{e-1}) = 2^{e-1} + 1$.

If G *is of type* III, *then* $C(F(\alpha)/F, 2^{e-1}) = 2^{e-2} + 1$.

Proof. If G is of type IV, then by Lemma 3.9, H_1 and H_3 are cyclic subgroups and they both contain the subgroup $\langle A^2 \rangle$. However, $|H_2| = 2^{e-1}$, and $H_2 = \langle A^2, B \rangle \cong Z_{2^{e-2}} \oplus Z_2$. Therefore, it is sufficient to count the subgroups of H_2 and this group has three different subgroups of each order.

If G is of type III, then by Lemma 3.9, H_2 is a dihedral group and H_3 is a generalized quaternion, so we will count first the number of subgroups of the groups of type I and type II. The proof goes by induction, observing that if $H \leqslant G$, then H is a cyclic group or H and G are of the same type, by Lemma 3.9. Also $H \subseteq H_i$, for some $i = 1, 2, 3$, by Lemma 3.7, and if $|G : H| = 2^k$, then H is contained in a subgroup of G of index 2^{k-1}.

If $k = 1$, then the number of subgroups of index 2 in G is 3, by Lemma 3.7, where one of these subgroups is cyclic. Assume that the number of subgroups of index 2^k is $2^k + 1$, where $1 \leqslant k \leqslant e-3$. To count the number of subgroups of index 2^{k+1}, it is sufficient to count the number of subgroups of index 2 in each subgroup of index 2^k. Let H be a non-cyclic subgroup of index 2^k, then H contains three subgroups G_i, $i = 1, 2, 3$, with $[G : G_i] = 2^{k+1}$, $G_1 = \langle A^{2^k} \rangle$, and G_2, G_3 not contained in any other subgroup of index 2^k. Thus the number of subgroups of index 2^{k+1} is $2(2^k + 1 - 1) + 1 = 2^{k+1} + 1$. To count the number of subgroups of index 2^{e-1}, observe that a generalized quaternion has a unique element of order 2, and a dihedral group of order 2^e has $2^{e-1} + 1$ involutions.

For the group G of type III, the above argument works for the case $1 \leqslant k \leqslant e-2$. For $k = e-1$, note that H_1 and H_3 contain a unique involution, $A^{2^{e-2}}$, which is also contained in H_2, a dihedral group with $2^{e-2} + 1$ involutions. ∎

4. ROOTS OF IRREDUCIBLE BINOMIALS IN RADICAL EXTENSIONS

In this section we consider which subextensions of $F(\alpha)/F$ are defined by a root of an irreducible binomial and how such binomials are related to $x^m - a$. Specifically we characterize $B(F(\alpha)/F) = \{\beta \in F(\alpha) : |F(\beta) : F| = O_F(\beta)\}$, the set of elements of $F(\alpha)$ which satisfy irreducible binomials over

F, describe the irreducible binomials over F with roots in $F(\alpha)$, and classify them up to equivalence (defined in Section 1). As usual in these studies, the powers of 2 cause complications, as the next lemma indicates.

Recall the conventions introduced in Section 1. If m is even, then char $F \neq 2$. Also, in equations, small latin letters shall denote elements from F. Given m, we say that $a \sim b$ at m if there exists a $c \in F$ such that $a = b^i c^m$, $(i, j) = 1$.

LEMMA 4.1. *Let* $m = 2^e m_0$, $(m_0, 2) = 1$, *and* $\beta \in B(F(\alpha)/F)$, *then* $\beta = c\zeta_k(\alpha^{2^e})^i\bar{\beta}$, *where* $k \mid O_F((\alpha^{2^e})^i)$ *and* $\bar{\beta} \in B(F(\alpha^{m_0})/F)$.

Conversely, if $\bar{\beta} \in B(F(\alpha^{m_0})/F)$ *and* $\zeta_k \in F(\alpha)$ *such that* $k \mid O_F((\alpha^{2^e})^i)$, *then* $\zeta_k(\alpha^{2^e})^i\bar{\beta} \in B(F(\alpha)/F)$.

Proof. This representation is a direct result of Theorem A of [3]. ∎

In the following we may assume that $m_0 = 1$ since Lemma 4.1 reduces the problem of determining $B(F(\alpha)/F)$ to one of determining $B(F(\alpha^{m_0})/F)$. Further, if $\zeta_4 \notin F(\alpha)\backslash F$, then $T_2(F(\alpha)^*/F^*) = \langle aF^* \rangle$ $(m_0 = 1)$ so if $\beta \in B(F(\alpha)/F)$, $O_F(\beta) = 2^k$, then $\beta = c\alpha^{r2^{e-k}}$, $(r, 2) = 1$; thus $b = c^{2^k}a^r$. For char $F \neq 2$ and $\zeta_4 \notin F$ recall that $\eta_{2^t} = \zeta_{2^t} + \zeta_{2^t}^{-1}$ and $T = \max\{t: \eta_{2^t} \in F\}$ if the set is finite and $T = \infty$ otherwise. Furthermore, set $\varepsilon = 1$ if $T = \infty$ and $\varepsilon = (2 + \eta_{2^T})^{2^{T-2}}$ otherwise.

LEMMA 4.2. *Let* $x^4 - a$ *be irreducible over* F *with* $\zeta_4 \notin F$ (char $F \neq 2$). *Then* $F(\zeta_4) = F(a^{1/2})$ *iff* $-a \in F^2$. *Let* $-a \in F^2$, *then* $x^{2^k} \pm \varepsilon\sqrt{-a}$ *are irreducible for all* k. *Further,* $x^{2^k} - a$, $x^{2^k} - \varepsilon\sqrt{-a}$, $x^{2^k} + \varepsilon\sqrt{-a}$ *are mutually inequivalent.*

Proof. The first assertion is obvious and the irreducibility follows by applying Theorem 51 of [6]. If $\zeta_4 \in F(\sqrt{\pm\varepsilon\sqrt{-a}})$ then this would imply that one of $x^2 \pm \varepsilon\sqrt{-a}$ is reducible, a contradiction. Thus, $\zeta_4 \notin F(\sqrt{\pm\varepsilon\sqrt{-a}})$. However, if α is any root of $x^{2^k} - a$, then $\zeta_4 \in F(\alpha)$, which implies that $x^{2^k} - a$ is not equivalent to either $x^{2^k} \pm \varepsilon\sqrt{-a}$. Let $\beta_1^{2^k} = \varepsilon\sqrt{-a}$, $\beta_2^{2^k} = -\varepsilon\sqrt{-a}$, and suppose that $F(\beta_1) = F(\beta_2)$. Since $\zeta_4 \notin F(\beta_i)$, $i = 1, 2$, we have that $F(\beta_i)/F$ have the usp by Theorem 2.1. So the unique quadratic fields contained in these two fields must be the same. That is, $F(\sqrt{\varepsilon\sqrt{-a}}) = F(\sqrt{-\varepsilon\sqrt{-a}})$, which implies that $\zeta_4 \in F(\beta_i)$, a contradiction. Thus $F(\beta_1) \neq F(\beta_2)$ and the binomials are inequivalent. ∎

Set $R = \min\{e - 1, T - 1\}$.

THEOREM 4.1. *Let* $m = 2^e$, $\zeta_4 \in F(\alpha)\backslash F$, $\beta \in B(F(\alpha)/F)$, $\beta^{2^k} = b$, $k \leqslant e$. *If* $k \geqslant R + 1$, *then* $F(\beta) = F(\alpha^{2^{e-k}})$. *If* $k \leqslant R$, *then* $b \sim a$ *or* $b \sim \pm\varepsilon\sqrt{-a}$ *at* 2^k. *If* $k > R + 1$ *and* $e > T$, *then* $b \sim a$ *or* $b \sim (2 + \eta_{2^T})^{2^{k-1}}a$ *at* 2^k. *If* $F(\beta) = F(\alpha^{2^{e-k}})$ *and either* $k \leqslant R$ *or* $e \leqslant T$, *then* $b \sim a$ *at* 2^k. *Conversely,* $F(\alpha)$

contains the splitting fields of $x^{2^{R+1}} - a$, $x^{2^R} \pm \varepsilon\sqrt{-a}$. *Further, if* $k > R+1$ *and* $e > T$, *then* $F(\alpha)$ *contains a root of the irreducible binomial* $x^{2^k} - (2+\eta_{2^l})^{2^{k-1}}a$.

Proof. We first wish to show that if $k \geqslant R+1$, then $F(\beta) = F(\alpha^{2^{e-k}})$. If $e \leqslant T$, then $R = e-1$ and $k \geqslant R+1 = e$, so $k = e$ and the assertion is obvious. Thus we may assume that $T < e$, so $R = T-1$ and $k \geqslant T$.

Assume $\zeta_4 \notin F(\beta)$, then the order of β over $F(\zeta_4)$ is still 2^k and $F(\zeta_4, \beta) = F(\alpha^{2^{e-k-1}})$, since $F(\alpha)/F(\zeta_4)$ has the usp. By Theorem A of [3], $\beta = \gamma\alpha^{r2^{e-k-1}}$, where $\gamma \in F(\zeta_4)$, $(r, 2) = 1$. Thus $b = \beta^{2^k} = \gamma^{2^k}\alpha^{r2^{e-1}}$, so $\gamma^{2^k} \notin F$, yet $\gamma^{2^{k+1}} \in F$, so $O_F(\gamma) = 2^{k+1}$. However, by Corollary 1.2 of [3], $k+1 \leqslant T$, which contradicts the assumption that $k \geqslant T$. Hence if $k \geqslant T$, $\zeta_4 \in F(\beta)$, so $F(\beta) = F(\alpha^{2^{e-k}})$, since $F(\alpha)/F(\zeta_4)$ has the usp.

Let $\beta \in B(F(\alpha)/F)$, $O_F(\beta) = 2^k$, $b = \beta^{2^k}$. We consider two cases: (A) $\zeta_4 \in F(\beta)$ and (B) $\zeta_4 \notin F(\beta)$.

(A) If $\zeta_4 \in F(\beta)$, then $F(\beta) = F(\alpha^{2^{e-k}})$, so $\beta = \gamma\alpha^{r2^{e-k}}$, r odd, $\gamma \in F(\zeta_4)$, $O_F(\gamma) \leqslant 2^k$. By Theorem A of [3], if $T = \infty$, $T(F(\zeta_4)^*/F^*) = \langle \zeta_{2^l}F^*$: for all $t\rangle$ and if $T < \infty$, $T(F(\zeta_4)^*/F^*) = \langle (1+\zeta_{2^l})F^*\rangle \cong Z_{2^l}$. If $T = \infty$, then $\gamma = c\zeta_{2^l}$, $l \leqslant k+1$. If $l = k+1$, then $b = \beta^{2^k} = c^{2^k}(-1)\,a^r \in F^2$ since $-a \in F^2$ (recall $\zeta_4 \in F(\alpha)\backslash F$ iff $-a \in F^2$). Thus $l < k+1$ and $b = c^{2^k}a^r$; thus $b \sim a$ at 2^k. Hence we may assume that $T < \infty$. Thus $\gamma = c(1+\zeta_{2^l})^{i2^l}$, i odd.

Assume that $k > R+1$ and $e > T$. If $l > 0$, then $\gamma^{2^k} \in F^{2^k}$, so $b \sim a$ at 2^k. If $l = 0$, then $\gamma^{2^k} = c^{2^k}(2+\eta_{2^l})^{i2^{k-1}} = c_1^{2^k}(2+\eta_{2^l})^{2^{k-1}}$, for proper choice of c_1; thus $b \sim (2+\eta_{2^l})^{2^{k-1}}a$ at 2^k.

Assume that $k \leqslant R$ or $e \leqslant T$. As before, if $l > 0$, then $\gamma^{2^k} \in F^{2^k}$, so $b \sim a$ at 2^k. If $l = 0$, then $\gamma^{2^k} = c^{2^k}\zeta_{2^l}^{i2^{k-1}}(2+\eta_{2^l})^{i2^{k-1}}$, so $T-1 \leqslant k-1$, since $\zeta_4 \notin F$. If $T-1 = k-1$, then $b = c^{2^k}(2+\eta_{2^l})^{i2^{k-1}}(-1)\,a^r \in F^2$, a contradiction. Thus $T < k$. By assumption if $e > T$, then $k \leqslant R = T-1$, which contradicts $T < k$. Thus $e \leqslant T$ and $T < k$ imply that $e < k$, again a contradiction since $\beta \in F(\alpha)$; thus $k \leqslant e$. Hence $l \neq 0$.

(B) $\zeta_4 \notin F(\beta)$. Then $F(\beta, \zeta_4) = F(\alpha^{2^{e-k-1}})$, so $\beta = \gamma\alpha^{r2^{e-k-1}}$, r odd, $\gamma \in F(\zeta_4)$, and $b = \gamma^{2^k}\alpha^{r2^{e-1}} \in F$; thus $\gamma^{2^k} \notin F$, but $\gamma^{2^{k+1}} \in F$, so $O_F(\gamma) = 2^{k+1}$. If $T = \infty$, then $\gamma = c\zeta_{2^{k+2}}$; thus $b = c^{2^k}\alpha^{r2^{e-1}}\zeta_4 = c_1^{2^k}\zeta_4\sqrt{a} = c_1^{2^k}\sqrt{-a}$ for proper choice of c_1; thus $b \sim \pm\sqrt{-a}$ at 2^k. Hence, we can assume that $T < \infty$. Then $\gamma = c(1+\zeta_{2^l})^{i2^l}$, so $b = c^{2^k}(1+\zeta_{2^l})^{i2^{l+k}}\alpha^{r2^{e-1}} = c^{2^k}\zeta_{2^l}^{i2^{l+k}}(2+\eta_{2^l})^{i2^{l+k-1}}\alpha^{r2^{e-1}}$. Since $\alpha^{r2^{e-1}} \notin F$, we have that $\zeta_{2^l}^{i2^{l+k-1}} \notin F$, yet $\zeta_{2^l}^{i2^{l+k}} \in F$, so $l+k-1 = T-2$. Thus $b = c_1^{2^k}(2+\eta_{2^l})^{2^{T-2}}\sqrt{-a}$, for proper choice of c_1; hence $b \sim \pm(2+\eta_{2^l})^{2^{T-2}}\sqrt{-a}$ at 2^k.

Now, to prove the converse. Suppose $k > R+1$ and $e > T$ and suppose $b = (2+\eta_{2^l})^{2^{k-1}}a$, then $F(b^{1/2}) = F(a^{1/2}) = F(\zeta_4)$; thus $\zeta_4 \in F(\beta)$, where $\beta^{2^k} = b$. For some i, $\beta = \alpha^{2^{e-k}}\sqrt{2+\eta_{2^l}}\zeta_{2^k}^i = \alpha^{2^{e-k}}(\eta_{2^{l+1}})\zeta_{2^k}^i$. It is not the case that $F(\beta) = F(\alpha^{2^{e-k}})$, for all choices of i. However, since $(\zeta_{2^{l+1}})\eta_{2^{l+1}} = 1+\zeta_{2^l}$, and $k \geqslant T+1$, there must exist an i such that $(\eta_{2^{l+1}})\zeta_{2^k}^i =$

$1+\zeta_{2^T}\in F(\alpha)$, and this implies that, for this choice of i, $F(\beta)=F(\alpha^{2^{e-k}})$; thus $F(\alpha)$ contains a root of $x^{2^k}-(2+\eta_{2^T})^{2^{k-1}}a$.

Since $\eta_{2^T}\in F$, $\zeta_{2^T}\in F(\zeta_4)$. Thus $F(\alpha)$ contains the splitting field of $x^{2^{R+1}}-a$. If $T=\infty$, then $\varepsilon=1$ and $(\zeta_{2^{e+1}}\alpha)^{2^{e-1}}=\sqrt{-a}$ and $(\alpha\zeta_{2^{e+1}}^3)^{2^{e-1}}=-\sqrt{-a}$, so $F(\alpha)$ contains the roots of $x^{2^{e-1}}\pm\sqrt{-a}$. Assume now that $T<\infty$.

If $e\geqslant T$, set $\beta_1=(1+\zeta_{2^T})\alpha^{2^{e-T}}$, and $\beta_2=(1+\zeta_{2^T})^3\alpha^{2^{e-T}}$, then $\beta_1^{2^{T-1}}=(2+\eta_{2^T})^{2^{T-2}}\sqrt{-a}$ and $((2+\eta_{2^T})^{-1}\beta_2)^{2^{T-1}}=-(2+\eta_{2^T})^{2^{T-2}}\sqrt{-a}$. If $e<T$, set $\beta_1=(1+\zeta_{2^T})^{2^{T-e}}\alpha$ and $\beta_2=((1+\zeta_{2^T})^{2^{T-e}})^3\alpha$, then $\beta_1^{2^{e-1}}=(2+\eta_{2^T})^{2^{T-2}}\sqrt{-a}$ and $((2+\eta_{2^T})^{-2^{T-e}}\beta_2)^{2^{e-1}}=-(2+\eta_{2^T})^{2^{T-2}}\sqrt{-a}$. So $F(\alpha)$ contains all of the roots of $x^{2^R}\pm(2+\eta_{2^T})^{2^{T-2}}\sqrt{-a}$. ∎

THEOREM 4.2. *Suppose x^k-b is irreducible, $\beta^k=b$, $\beta\in F(\alpha)$, $k=2^{e_1}k_0$, k_0 odd. Then $F(\beta)=F(\alpha^{m/k}\zeta_{k_0}^i)$ iff either $\zeta_4\notin F(\alpha)\backslash F(\beta)$ or $e_1=0$. Further,* (i) *if $\zeta_4\in F(\beta)$ and $b\not\sim a$ at k, then $T<\infty$, $2^{T+1}\mid k$, and $b\sim(2+\eta_{2^T})^{k/2}a$ at k.* (ii) *If $\zeta_4\notin F(\beta)$ then $2^{R+1}\nmid k$ and $b\sim(\pm\varepsilon\sqrt{-a})^{k_0}a^{2^{e_1}}$ at k.*

Proof. By Theorem 2.3 we can see that $F(\beta)=K_1(\alpha^{m/k_0}\zeta_{k_0}^i)$, for some i, where K_1 is the unique subfield of $F(\beta)$ of degree 2^{e_1} over F. If $e_1=0$, then $K_1=F$ and the assertion is obvious. Thus assume $e_1>0$ and $\zeta_4\notin F(\alpha)\backslash F(\beta)$. If $\zeta_4\notin F(\alpha)\backslash F$, then $K_1=F(\alpha^{m/2^{e_1}})$ and the result follows. If $\zeta_4\in F(\alpha)\backslash F$, then $\zeta_4\in F(\beta)$ and again $K_1=F(\alpha^{m/2^{e_1}})$. Conversely, if $F(\beta)=F(\alpha^{m/k}\zeta_{k_0}^i)$ and $e_1>0$, then $F(\beta)\supset F(\alpha^{m/2^{e_1}})\supset F(\zeta_4)$, if $\zeta_4\in F(\alpha)\backslash F$; thus $\zeta_4\notin F(\alpha)\backslash F(\beta)$.

(i) Assume $\zeta_4\in F(\beta)$ and $b\not\sim a$ at k, then $F(\beta^{k_0})=F(\alpha^{m/2^{e_1}})\supset F(\zeta_4)$. Since $F(\beta)\supset F(\alpha^{m/k_0}\zeta_{k_0}^i)$, it follows that $b\sim a$ at k_0. However, since $b\not\sim a$ at k, we have that $b\not\sim a$ at 2^{e_1}. Now, by Theorem 4.1, we have that $T<\infty$, $e_1\geqslant T+1$, and $b\sim(2+\eta_{2^T})^{2^{e_1-1}}a$ at 2^{e_1}. A little calculation then yields that $b\sim(2+\eta_{2^T})^{k/2}a$ at k.

(ii) Now, let us assume that $\zeta_4\notin F(\beta)$. Then $2^{R+1}\nmid k$, by Theorem 4.1. Further $\beta^{2^{e_1}}=c_2(\alpha^{m/k_0})^{r_2}$, $(r_2,k_0)=1$, and $\beta^{k_0}=c_1(h^{1/2^{e_1}})^{r_1}$, $(r_1,2^{e_1})=1$, where $h=\pm\varepsilon\sqrt{-a}$. Choose x,y so that $xr_2=1+\lambda_1k_0$, $r_1y=1+2^{e_1}\lambda_2$, then for $l=2^{e_1}x+k_0y$, we have that $(l,k)=1$. Then $\beta^l=\beta^{x2^{e_1}}\beta^{k_0y}=c_3(\alpha^{m/k_0})^{xr_2}(h^{1/2^{e_1}})^{yr_1}$, where $c_3=c_1^yc_2^x$. Thus $b^l=(\beta^l)^k=c_3^k(a^{xr_2})^{2^{e_1}}(h^{yr_1})^{k_0}=c^ka^{2^{e_1}}h^{k_0}$, where $c=c_3a^{\lambda_1}h^{\lambda_2}$.

Hence, $b\sim a^{2^{e_1}}h^{k_0}$, at k, where h is as above. ∎

As a special case of Theorem 4.2, namely, when $k=m$, we can obtain the characterization of equivalent binomials which is due to Schinzel [10].

COROLLARY 4.1. *Assume that x^m-a, x^m-b are irreducible binomials with* char $F\nmid m$, *and $ab^{-t}\notin F^m$ for all t prime to m. Then $x^m-a\sim x^m-b$ iff $\zeta_4\in F(\alpha)\backslash F$, $T<\infty$, $2^{T+1}\mid m$, and $b^t=c^m(2+\eta_{2^T})^{m/2}a$, for some t prime to m.* ∎

We will now use the results of Sections 3 and 4 to characterize those binomials $x^{2^e} - a$ which are irreducible and normal, over fields of characteristic different from 2, and their corresponding Galois groups.

If $\zeta_4 \in F$, set $A = \max\{t: \zeta_{2^t} \in F\}$ if the set is finite, otherwise set $A = \infty$. Set $G = \mathrm{Gal}(F(\alpha)/F)$, for $\alpha^{2^e} = a$ and $x^{2^e} - a$ irreducible and normal.

THEOREM 4.3. *Let F be a field with* $\mathrm{char}\, F \neq 2$ *and $e \geqslant 3$. Then $x^{2^e} - a$ is irreducible and normal over F iff one of the following conditions holds.*

(A) $\zeta_4 \in F$. (i) $e \leqslant A$ *and* $a \notin F^2$ *or* (ii) $e > A$ *and* $a = c^{2^e} b^{2^{e-1}} \zeta_{2^A}$. *In both of these cases* $G = Z_{2^e}$.

(B) $\zeta_4 \notin F$. (i) $T = 2$, $\sqrt{-2} \notin F$, *then either* $a = -b^{2^{e-1}} c^{2^e}$ *and* $G = Z_2 \oplus Z_{2^{e-1}}$, *or* $e \geqslant 4$, $a = -b^{2^{e-1}} 2^{2^{e-2}} c^{2^e}$, *and G is of type* IV. (ii) $T = 2$, $\sqrt{-2} \in F$, *then* $e = 3$, $a = -b^2 c^8$, $4b^2 \notin F^4$, *and G is the quaternion group.* (iii) $T > 2$, $\zeta_4 \eta_{2^{T+1}} \notin F$, *and* $e \leqslant T + 1$. *Then* $e = T + 1$ *iff* $a = -(2 + \eta_{2^1})^2 c^{2^e}$ *or* $a = -(2 + \eta_{2^T})^2 (2 + \eta_{2^T})^{2^{e-2}} c^{2^e}$, *and G is of type* III. *If* $e \leqslant T$ *then* $a = -b^2 c^{2^e}$, $b^2 \notin F^4$, *and G is the dihedral group.* (iv) $T > 2$, $\zeta_4 \eta_{2^{T+1}} \in F$, *and* $e \leqslant T + 1$. *Then* $e = T + 1$ *iff* $a = -b^2 (2 + \eta_{2^T})^{2^{e-2}} c^{2^e}$ *or* $a = -b^2 c^{2^e}$, *where* $b^2 \notin F^4$ *and G is the quaternion group. If* $e \leqslant T$, *then* $a = -b^2 c^{2^e}$, $b^2 \notin F^4$, *and G is the dihedral group.* (v) $T = \infty$, $a = -b^2 c^{2^e}$, $b^2 \notin F^4$, *and G is the dihedral group.*

Proof. (A) $\zeta_4 \in F$. (i) If $e \leqslant A$, then $\zeta_{2^e} \in F$, so $x^{2^e} - a$ is irreducible and normal iff $x^{2^e} - a$ is irreducible and this occurs iff $a \notin F^2$.

(ii) if $e > A$, then $x^{2^e} - a$ is normal iff $\zeta_{2^e} \in F(\alpha)$. However, $|F(\zeta_{2^e}) : F| = 2^{e-A}$; thus $F(\alpha^{2^A}) = F(\zeta_{2^e})$, so $\alpha^{2^A} = b\zeta_{2^e}$, and $a = \alpha^{2^e} = (\alpha^{2^A})^{2^{e-A}} = (b\zeta_{2^e})^{2^{e-A}} = b^{2^{e-A}} \zeta_{2^A} \notin F^2$, since $\zeta_{2^A} \notin F^2$. In both cases $F(\alpha)/F$ has the usp, so G is cyclic.

(B) $\zeta_4 \notin F$. The extension is normal iff $\zeta_{2^e} \in F(\alpha)$. (i) $T = 2$, $\sqrt{-2} \notin F$, then $|F(\zeta_{2^e}) : F| = 2^{e-1}$. Thus $F(\alpha)/F$ is normal iff $F(\alpha^2) = F(\zeta_{2^e})$. Also α^2, ζ_{2^e} satisfy the irreducible binomials $x^{2^{e-1}} - a$, $x^{2^{e-1}} + 1$, respectively; thus $x^{2^{e-1}} - a \sim x^{2^{e-1}} + 1$, so we can apply Corollary 4.1.

If $e - 1 = 2$, then $a = (-1) b^4$, so $x^8 - a = x^8 + b^4$.

If $e - 1 \geqslant 3$, then $a = (-1) b^{2^{e-1}}$ or $a = (-1) b^{2^{e-1}} 2^{e-2}$. If $a = (-1) b^{2^{e-1}}$ then G is $Z_2 \oplus Z_{2^{e-1}}$. If $a = (-1) b^{2^{e-1}} 2^{e-2}$ then G is not abelian (Theorem 2.1 of [11]), so G must be of type IV.

(ii) $T = 2$, $\sqrt{-2} \in F$. By Lemma 3.3, $\zeta_{2^4} \notin F(\alpha)$, so $e \leqslant 3$, yet $e \geqslant 3$, by assumption, thus $e = 3$. Since $F(\zeta_4) = F(\zeta_8)$, we have that $F(\alpha^4) = F(\zeta_4)$; thus $\alpha^4 = b\zeta_4$, $a = -b^2$. In order for $x^4 - a$ to be irreducible we must have that $-4a = 4b^2 \notin F^4$. By Lemma 3.2, G is not abelian and in fact, G is the generalized quaternion group by Corollary 3.1.

(iii) $T > 2$, $\zeta_4 \eta_{2^{T+1}} \notin F$. By Lemma 3.4 we have that $e \leqslant T + 1$. Further

$e = T + 1$ iff $a \sim -(2 + \eta_{2^T})^2$ at 2^2, so $a = -(2 + \eta_{2^T})^2 c^{2^e}$ or $a = -(2 + \eta_{2^T})^2 (2 + \eta_{2^T})^{2^{e-2}} c^{2^e}$ by Theorem 4.2. By Lemma 3.5, G is of type III.

If $e \leqslant T$, then $F(\alpha)/F$ is normal iff $F(a^{1/2}) = F(\zeta_4) = F(\zeta_{2^e})$, since $e \leqslant T$, thus $a^{1/2} = b\zeta_4$, $a = -b^2$. To insure that $x^4 - a$ is irreducible, we must have that $-4a = 4b^2 \notin F^4$. But this is equivalent to $b^2 \notin F^4$ since $\sqrt{2} \in F$. By Corollary 3.1, G is the dihedral group.

(iv) $T > 2$, $\zeta_4 \eta_{2^{T+1}} \in F$. By Lemma 3.3, $e \leqslant T + 1$. Further, $F(\alpha)/F$ is normal iff $F(a^{1/2}) = F(\zeta_4) = F(\zeta_{2^e})$ since $e \leqslant T + 1$. Thus, $a^{1/2} = b\zeta_4$, $a = -b^2$, and $b^2 \notin F^4$ to ensure that $x^4 - a$ is irreducible.

If $e = T + 1$, then $a \sim -b^2$ at 2 implies that $a = -b^2 c^{2^e}$ or $a = -b^2 (2 + \eta_{2^T})^{2^{e-2}} c^{2^e}$, by Theorem 4.2, and G is the generalized quaternion by Corollary 3.1.

If $e < T + 1$, then $a \sim -b^2$ at 2 implies that $a = -b^2 c^{2^e}$ and G is the dihedral group, by Corollary 3.1.

(v) $T = \infty$, then $F(\alpha)/F$ is normal iff $F(a^{1/2}) = F(\zeta_4) = F(\zeta_{2^e})$, since $T = \infty$. Thus $a = -b^2$ and to ensure that $x^4 - a$ is irreducible we must have that $b^2 \notin F^4$. Thus $a = -b^2 c^{2^e}$ and G is the dihedral group by Corollary 3.1. ∎

REFERENCES

1. D. GAY, On normal radical extensions of real fields, *Acta Arith.* **35** (1979), 273–288.
2. D. GAY, Normal binomials over algebraic number fields, *J. Number Theory* **12** (1980), 311–326.
3. D. GAY AND W. YSLAS VÉLEZ, The torsion group of a radical extension, *Pacific J. Math.* **92** (1981), 317–327.
4. I. GERST, On the theory of nth power residues and a conjecture of Kronecker, *Acta Arith.* **17** (1970), 121–139.
5. M. HALL, JR., "The Theory of Groups," Macmillan Co., New York, 1959.
6. I. KAPLANSKY, "Fields and Rings," 2nd ed., Univ. Chicago Press, Chicago/London, 1972.
7. H. MANN AND W. YSLAS VÉLEZ, On normal radical extensions of the rationals, *J. of Lin. and Multilin. Alg.* **3** (1975), 73–80.
8. G. A. MILLER, H. F. BLICHFELDT, AND L. E. DICKSON, "Theory and Applications of Finite Groups," Dover, New York, 1961.
9. M. NORRIS AND W. YSLAS VÉLEZ, Structure theorems for radical extensions of fields, *Acta Arith.* **37** (1980), 111–115.
10. A. SCHINZEL, On linear dependence of roots, *Acta Arith.* **28** (1975), 161–175.
11. W. YSLAS VÉLEZ, On normal binomials, *Acta Arith.* **36** (1980), 113–124.
12. H. ZASSENHAUS, "The Theory of Groups," 2nd ed., Chelsea, New York, 1958.